

NTP en el ejemplo de configuración de los reguladores del Wireless LAN

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Manejo de la fecha del sistema y del tiempo en el regulador del Wireless LAN](#)

[Configurar](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

Este documento explica cómo configurar los reguladores del Wireless LAN (WLCs) para sincronizar la fecha y hora con un servidor del Network Time Protocol (NTP).

[prerrequisitos](#)

[Requisitos](#)

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento básico de la configuración de los Puntos de acceso ligeros (revestimientos) y del WLCs de Cisco
- Conocimiento básico del NTP

[Componentes Utilizados](#)

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WLC de Cisco 4400 que funciona con la versión de software 7.0.116.0
- Revestimientos de las Cisco 1230AG Series
- Cisco 2800 Series Router que funciona con el Software Release 12.4(11)T de Cisco IOS®

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

[Convenciones](#)

Consulte [Convenciones de Consejos Técnicos Cisco](#) para obtener más información sobre las convenciones del documento.

[Manejo de la fecha del sistema y del tiempo en el regulador del Wireless LAN](#)

En un WLC, la fecha del sistema y el tiempo se pueden configurar manualmente del WLC o configurar para obtener la fecha y hora de un servidor NTP.

La fecha del sistema y el tiempo se pueden configurar manualmente usando el Asistente o el WLC GUI/CLI de la configuración CLI. Este documento proporciona un ejemplo de configuración para sincronizar la fecha del sistema y el tiempo del WLC a través de un servidor NTP.

El NTP es un protocolo de Internet usado para sincronizar los relojes de los ordenadores a una cierta referencia de tiempo. [El RFC 1305](#) proporciona la información detallada en la implementación del v3 NTP. [Una red NTP recibe generalmente su tiempo de una fuente de tiempo válida, tal como una radio reloj o un reloj atómico asociado a un Servidor de tiempo. El NTP entonces distribuye este vez a través de la red. Un cliente NTP hace una transacción con su servidor sobre el intervalo de sondeo \(a partir 64 a 1024 segundos\), que cambia dinámicamente en un cierto plazo dependiendo de los estados de la red entre el servidor NTP y el cliente. La otra situación ocurre cuando el router comunica a un mún servidor NTP \(por ejemplo, servidor NTP con la dispersión grande\). El router también aumenta el intervalo de encuesta. No más que una transacción NTP por el minuto es necesaria sincronizar dos máquinas. No es posible ajustar el intervalo de encuesta NTP en un router.](#)

El NTP utiliza el concepto de un estrato para describir cuántos saltos NTP lejos es una máquina de una fuente de tiempo válida. Por ejemplo, un Servidor de tiempo del estrato 1 tiene una radio o un reloj atómico asociado directamente a él. Entonces envía su tiempo a un Servidor de tiempo del estrato 2 con el NTP, y así sucesivamente.

Para más información sobre las mejores prácticas para el despliegue NTP, refiera al [protocolo Network Time Protocol: White Paper de las mejores prácticas](#). El ejemplo en este documento utiliza a un Cisco 2800 Router como servidor NTP. El WLC se configura para sincronizar su fecha y hora con este servidor NTP.

[Configurar](#)

[Configurar al Cisco 2800 Series Router como servidor NTP](#)

Configurar al router como servidor NTP autoritario

Utilice este comando en el modo de configuración global si usted quisiera que el sistema fuera servidor NTP autoritario, incluso si el sistema no se sincroniza a una fuente horaria exterior:

```
ntp master
!--- Makes the system an authoritative NTP server
```

El configurar autenticación NTP

Si usted quiere autenticar las asociaciones con otros sistemas por motivos de seguridad, utilice los comandos que siguen. El primer comando habilita autenticación NTP la característica. El comando `second` define cada uno de las claves de autenticación. Cada clave tiene un número dominante, un tipo, y un valor. Actualmente, el único tipo dominante soportado es md5. Tercero, una lista de “confiaba en que” las claves de autenticación están definidas. Si se confía en una clave, este sistema estará listo para sincronizar a un sistema que utilice esta clave en sus paquetes NTP. Para configurar autenticación NTP, utilice estos comandos en el modo de configuración global:

```
ntp authenticate
!--- Enables the NTP authentication feature ntp authentication-key number md5 value !--- Defines
the authentication keys ntp trusted-key key-number !--- Defines trusted authentication keys
```

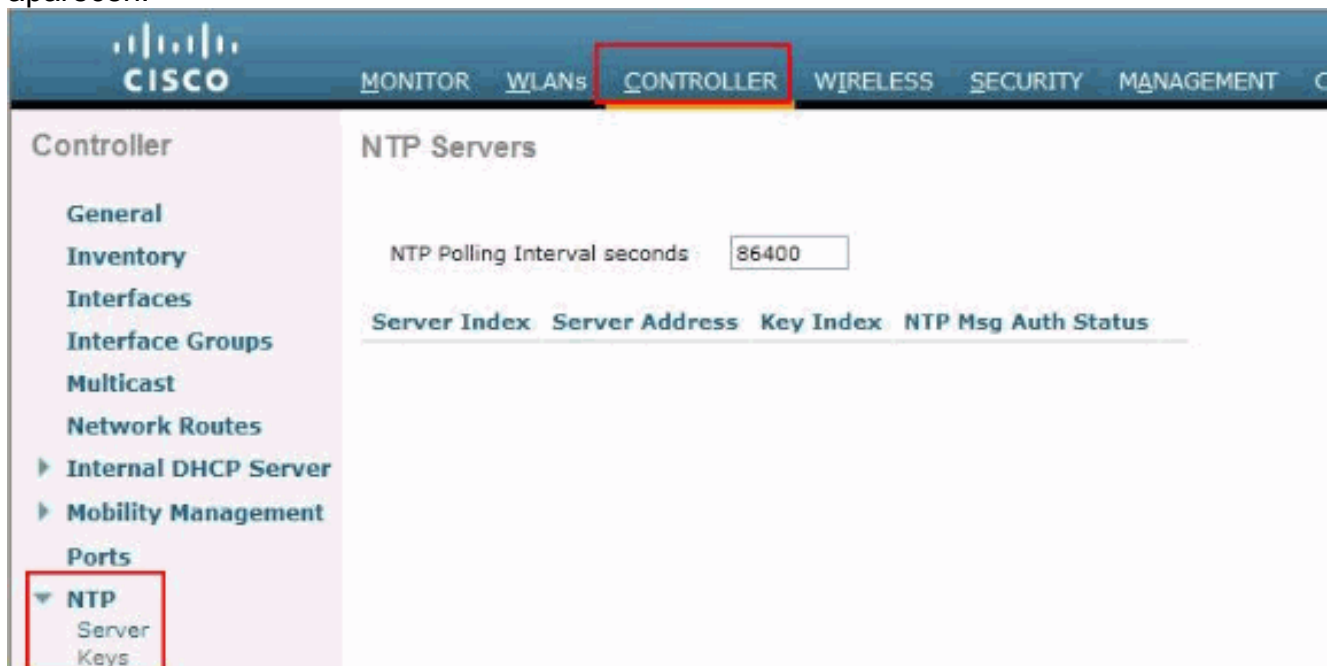
Aquí está una configuración de servidor NTP del ejemplo en el 2800 Series Router. El router es el master NTP, que significa que el router actúa como el servidor NTP autoritario.

```
ntp master
ntp authenticate
ntp authentication-key 1 md5 0305480F0008 7
ntp trusted-key 1
```

[Configurar el WLC para el servidor NTP](#)

Comenzando con la versión de 7.0.116.0, usted puede también configurar un canal de la autenticación entre el regulador y el servidor NTP. Para configurar autenticación NTP usando el regulador GUI, realice estos pasos:

1. Elija el **regulador > el NTP > los servidores** para abrir la página de los servidores NTP. Haga clic **nuevo** para agregar a un servidor NTP. **Los servidores NTP > nueva página** aparecen.



2. Elija una prioridad del servidor de la lista desplegable del **índice del servidor (prioridad)**.
3. Ingrese el IP Address del servidor NTP en el cuadro de texto del **IP address del servidor**.
4. Habilite la autenticación de servidor NTP seleccionando la casilla de verificación de la

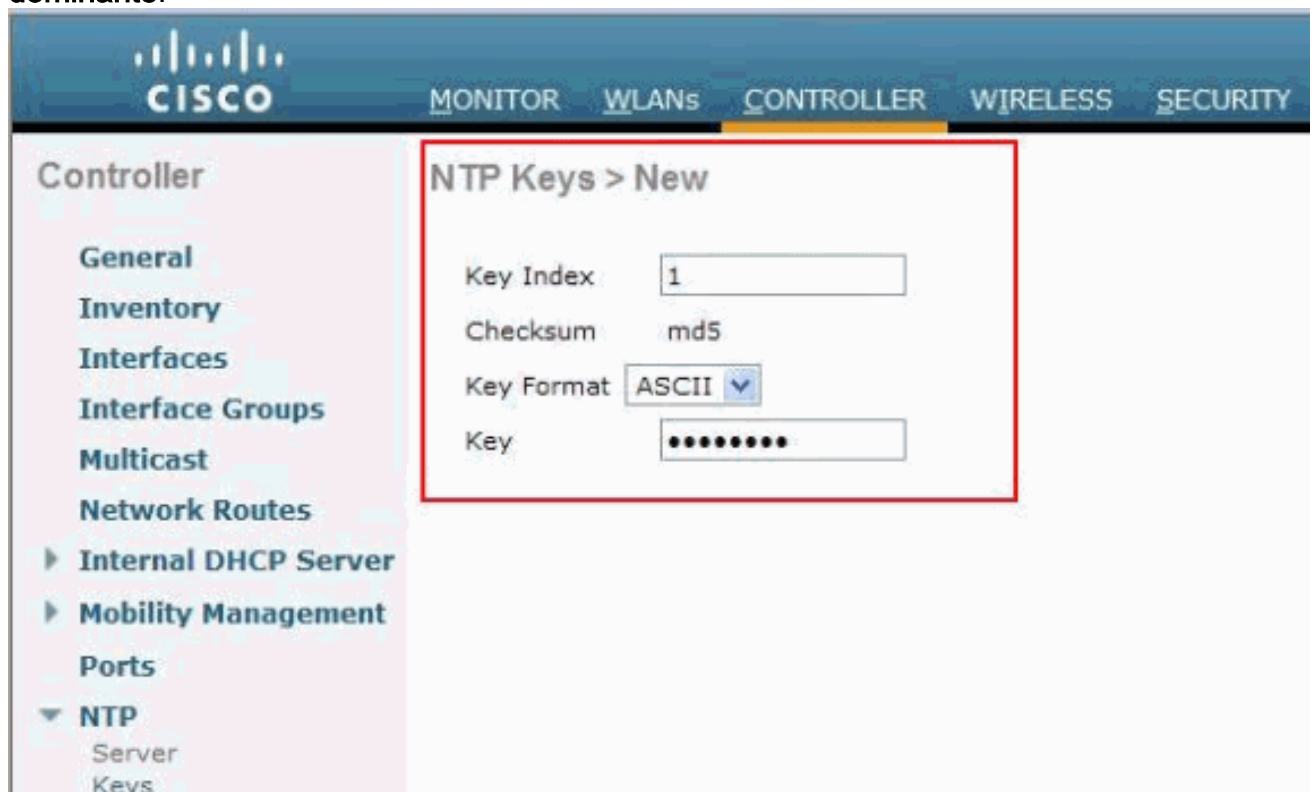
autenticación de servidor
NTP.



The screenshot shows the Cisco NTP Servers configuration page. The left sidebar contains a navigation menu with the following items: General, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, and NTP (expanded to show Server and Keys). The main content area is titled "NTP Servers > New" and contains the following fields:

Server Index (Priority)	1
Server IP Address	10.78.177.30
Enable NTP Authentication	<input checked="" type="checkbox"/>
Key Index	1

5. Haga clic en Apply (Aplicar).
6. Elija el **regulador > el NTP > las claves**.
7. Haga clic **nuevo** para crear una clave.
8. Ingrese el índice dominante en el cuadro de texto del **índice dominante**.
9. Elija el formato dominante de la lista desplegable **dominante del formato**.
10. Ingrese la clave en el cuadro de texto **dominante**.



The screenshot shows the Cisco NTP Keys configuration page. The left sidebar is identical to the previous screenshot. The main content area is titled "NTP Keys > New" and contains the following fields:

Key Index	1
Checksum	md5
Key Format	ASCII
Key

Verificación

Usted puede utilizar estos comandos del WLC CLI de verificar la configuración:

```
(Cisco Controller) >show time Time..... Wed Nov 23
15:31:27 2011 Timezone delta..... 0:0 Timezone
location..... (GMT -6:00) Central Time (US and Canada) NTP Servers
NTP Polling Interval..... 86400 Index NTP Key Index NTP Server NTP Msg Auth
Status ----- 1 1 10.78.177.30
AUTH SUCCESS
```

Troubleshooting

Usted puede utilizar el **comando enable del detalle NTP del debug** de ver la Secuencia de eventos que ocurre la configuración de servidor NTP se hace una vez en el WLC.

```
*sntpReceiveTask: Nov 23 15:08:24.360: Started=3531049704.360568 2011 Nov 23 15:08:24.360
*sntpReceiveTask: Nov 23 15:08:24.360: Looking for the socket addresses
*sntpReceiveTask: Nov 23 15:08:24.360: NTP Polling cycle: accepts=0, count=5, attempts=1,
retriesPerHost=6.
  Outgoing packet on NTP Server on socket 0:
*sntpReceiveTask: Nov 23 15:08:24.360: sta=0 ver=3 mod=3 str=15 pol=8 dis=0.000000 ref=0.000000
*sntpReceiveTask: Nov 23 15:08:24.361: ori=0.000000 rec=0.000000
*sntpReceiveTask: Nov 23 15:08:24.361: tra=3531049704.360889 cur=3531049704.360889
*sntpReceiveTask: Nov 23 15:08:24.361: Host Supports NTP authentication with Key Id = 1
*sntpReceiveTask: Nov 23 15:08:24.361: NTP Auth Key Id = 1 Key Length = 5
*sntpReceiveTask: Nov 23 15:08:24.361: MD5 Hash and Key Id added in NTP Tx packet
*sntpReceiveTask: Nov 23 15:08:24.361: Flushing outstanding packets
*sntpReceiveTask: Nov 23 15:08:24.361: Flushed 0 packets totalling 0 bytes
*sntpReceiveTask: Nov 23 15:08:24.361: Packet of length 68 sent to 10.78.177.30 UDPport=123
*sntpReceiveTask: Nov 23 15:08:24.363: Packet of length 68 received from 10.78.177.30
UDPport=123
*sntpReceiveTask: Nov 23 15:08:24.363: KeyId In Recieved NTP Packet 1
*sntpReceiveTask: Nov 23 15:08:24.363: KeyId 1 found in recieved NTP packet exists as part of
the trusted Key/s
*sntpReceiveTask: Nov 23 15:08:24.363: The NTP trusted Key Id 1 length = 5
*sntpReceiveTask: Nov 23 15:08:24.363: NTP Message Authentication - SUCCESS *sntpReceiveTask:
Nov 23 15:08:24.363: sta=0 ver=3 mod=4 str=8 pol=8 dis=3.875031 ref=3531071269.384065
*sntpReceiveTask: Nov 23 15:08:24.363: ori=3531049704.360889 rec=3531071270.103183
*sntpReceiveTask: Nov 23 15:08:24.363: tra=3531071270.103387 cur=3531049704.363251
```

Información Relacionada

- [Protocolo Network Time Protocol: Informe oficial de Mejores Prácticas](#)
- [Guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco, versión 7.0.116.0](#)

- [Soporte Técnico y Documentación - Cisco Systems](#)